

SoK: The Past Decade of User Deception in Emails and Today's Email Clients' Susceptibility to Phishing Techniques

Maxime Veit
Karlsruhe Institute of Technology
maxime.veit@kit.edu

Oliver Wiese
CISPA Helmholtz Center for
Information Security
oliver.wiese@cispa.de

Fabian Lucas Ballreich
Karlsruhe Institute of Technology
fabian.ballreich@kit.edu

Melanie Volkamer
Karlsruhe Institute of Technology
melanie.volkamer@kit.edu

Douglas Engels
Freie Universität Berlin
douglas.engels@fu-berlin.de

Peter Mayer
University of Southern Denmark /
Karlsruhe Institute of Technology
mayer@imada.sdu.dk

March 3, 2026

Abstract

User deception in emails is still one of the biggest security risks companies and end-users face alike. Attackers try to mislead their victims when assessing whether emails are dangerous to interact with, e.g., by using techniques based on dangerous links, dangerous attachments, or both. In this work, we present a systematic literature research of deception techniques discussed in the scientific literature of the last decade. We systematize the deception techniques, focusing on techniques that use misleading sender, link, and/or attachment information. We identify 23 deception techniques which we classify as either those that email clients should protect users against (13) and those that email clients cannot protect against and thus should be addressed in security awareness measures (10). We propose a security rating for the susceptibility of email

clients to these 13 deception techniques and perform an empirical evaluation to analyze the susceptibility of seven representative email clients (web, mobile apps, desktop apps) to these deception techniques. The results of our evaluation indicate that most email clients are in need of improvement to defend against the deception techniques. Hardening email clients against these deception techniques is necessary to increase the resistance against them – without unnecessarily burdening users.